Challenges of Electronic Contracts and Consumer Protection in Nigeria under the FCCPA 2018 and CAMA 2020

Chioma Chidera Ugwu
Department of Legal Studies
Akanu Ibiam Federal Polytechnic Unwana, Ebonyi State.

Abstract

This paper explores the legal challenges surrounding electronic contracts in Nigeria, particularly consumer protection under the Federal Competition and Consumer Protection Act (FCCPA) 2018 and the Companies and Allied Matters Act (CAMA) 2020. As digital platforms increasingly dominate commerce, from fintech to online retail, electronic contracting has become standard. Frameworks such as the Evidence (Amendment) Act 2023, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, NITDA guidelines, and the Nigeria Data Protection Act 2023 contribute to the regulatory landscape, but the FCCPA and CAMA remain pivotal. However, both Acts reveal significant gaps and ambiguities that compromise enforcement and consumer rights in digital transactions. Key findings include: (1) the FCCPA outlines progressive consumer rights and establishes the FCCPC as the principal enforcer, but lacks procedural clarity for online disputes and does not address challenges such as clickwrap agreements and digital identity fraud; (2) CAMA acknowledges electronic filing, but does not resolve questions concerning electronic signatures, corporate accountability, or transparency in online business models; (3) although other statutes provide partial safeguards, the legal framework remains fragmented; (4) enforcement is hindered by institutional overlap, limited technical expertise, and low consumer digital literacy; and (5) international models, including UK and EU frameworks, offer benchmarks for reform. The paper proposes statutory clarification of electronic consent, mandatory transparency for digital traders, sector-specific FCCPA guidance, enhanced corporate obligations under CAMA, unified standards for electronic signatures, expedited ODR mechanisms, and institutional capacity building. These reforms can reduce power imbalances, enhance consumer redress, and build trust in Nigeria's digital economy.

Keywords: Consumer rights, online transactions, digital contracts, e-commerce regulation, digital economy, data privacy.

Introduction

Electronic contracting, including offers, acceptances, and performance concluded wholly or partly by electronic means, is now an ordinary commercial practice in Nigeria. E-commerce platforms, digital payment systems, mobile apps, software-as-a-service, and online marketplaces have moved commercial bargaining into digital space, where traditional rules of contract formation, consumer protection, and corporate accountability are being tested in new ways. The rise of electronic contracts magnifies classic consumer-law problems, including information asymmetry, adhesion contracts, algorithmic profiling, and cross-border enforcement difficulties. For Nigeria, whose digital economy is expanding rapidly, the way courts, regulators, and firms treat electronic contracts will materially influence consumer trust, market growth, and the legal contours of commerce. The research problem is therefore as follows: Do current Nigerian statutes, particularly the Federal Competition and Consumer Protection Act (FCCPA) 2018 and the Companies and Allied Matters Act (CAMA) 2020, adequately protect consumers who enter into electronic contracts? If not, what doctrinal, institutional, and policy reforms are necessary to secure consumer rights while enabling digital commerce?

The specific objectives are to:

(a) map the relevant statutory architecture that governs online contracting and consumer protection;

(b) identify doctrinal ambiguities and enforcement gaps under FCCPA and CAMA;

(c) explore how complementary laws, including the Evidence Act 2011 (as amended by the Evidence (Amendment) Act 2023), the Cybercrimes Act 2015, NITDA instruments, and the NDPA 2023, interact with those statutes; and

(d) propose practicable reforms informed by comparative practice and doctrinal principles.

Methodology

The study doctrinally analyses primary legal materials (statutes, regulations, policy guidelines), reported cases and institutional reports; it then synthesises scholarly commentary and comparative legal practice. No empirical fieldwork is conducted; instead, the focus is legal interpretation, statutory construction and normative critique. The doctrinal approach is appropriate because the project concerns the content, coherence and application of legal rules governing electronic contracts and consumer protection. The analysis privileges textual interpretation, systemic coherence and the principle of pro-consumer construction where ambiguity threatens fundamental protections. Key primary sources included the FCCPA 2018 (the consumer-law statute and regulator's resources), the Companies and Allied Matters Act 2020 (CAMA), the Evidence Act 2011 (electronic evidence and signatures), Cybercrimes Act 2015 (digital offences), the NITDA Act and guidance, and the Nigeria Data Protection Act 2023 (privacy obligations for online contracting platforms) (FCCPA, 2018).

The article proceeds as follows. Section 2 clarifies key concepts, including electronic contracts, electronic signatures, clickwrap and browsewrap agreements, and consumer protection principles. Section 3 maps the statutory landscape, comprising the FCCPA 2018 and CAMA 2020, together with complementary instruments such as the Evidence Act 2011, the Cybercrimes Act 2015, NITDA guidance, and the NDPA 2023. Section 4 doctrinally analyses the FCCPA and CAMA against the realities of electronic contracting, highlighting gaps concerning consent, transparency, and remedies. Section 5 focuses on evidence and enforcement challenges, including proof of electronic assent, the weight of digital records, and jurisdictional and cross-border problems. Section 6 evaluates institutional capacity and inter-agency overlap among the FCCPC, CAC, NITDA, NDPC, and sectoral regulators. Section 7 draws comparative lessons and offers targeted recommendations concerning statutory drafting, sectoral guidance, ODR, and corporate compliance duties under CAMA. A concluding section summarises the paper's principal contributions and identifies areas for further research.

The article proceeds as follows. Section 2 clarifies key concepts: electronic contracts, e-signatures, clickwrap/browse wrap agreements, and consumer protection principles. Section 3 maps the statutory landscape (FCCPA 2018; CAMA 2020) and complementary instruments (Evidence Act 2011; Cybercrimes Act 2015; NITDA guidance; NDPA 2023). Section 4 doctrinally analyses the FCCPA and CAMA against the realities of electronic contracting, highlighting gaps on consent, transparency and remedies. Section 5 focuses on evidence and enforcement challenges: proof of electronic assent, the weight of digital records, jurisdictional and cross-border problems. Section 6 evaluates institutional capacity and inter-agency overlap (FCCPC, CAC, NITDA, NDPC, sectoral regulators). Section 7 draws comparative lessons and offers targeted recommendations (statutory drafting, sectoral guidance, ODR, corporate compliance duties under CAMA). A concluding section summarises original contributions and sets a research agenda. Throughout, the article uses APA-style sourcing and cites primary sources.

Why FCCPA 2018 and CAMA 2020?

Two statutes are central. The FCCPA 2018 consolidated consumer rights and created the Federal Competition and Consumer Protection Commission, with powers to investigate unfair practices, order remedies, and undertake consumer education, functions directly relevant to online trading. The Companies and Allied Matters Act 2020 modernised company law, recognised electronic filing and corporate digital processes, and established rules bearing on corporate conduct online, including directors' duties and corporate transparency. Together, they shape how businesses operate online and how consumers may seek redress. However, each statute was drafted in a transitional environment and did not fully anticipate algorithmic contracting, clickwrap defaults, or large-scale platform markets. This mismatch is the core problem addressed by the article.

Preliminary observations from primary sources

FCCPA 2018 provides an expansive set of consumer rights (right to information, safety, redress and fair treatment) and enforcement tools (administrative orders, fines, consumer education), but it lacks sector-specific rules for e-commerce and does not specify the technical modalities for proving electronic consent or automated contract formation. This creates enforcement friction when consumers complain about supposedly authorised online debits, dark patterns, or automated renewals. CAMA 2020 recognises electronic filing and permits electronic communications with the Corporate Affairs Commission. It enhances corporate regulation in ways that favour digital business. Yet corporate duties to consumers, including transparency in online terms, corporate governance responsibilities for digital platforms, and director oversight of consumer-facing algorithms, are not fully developed. This legislative gap places the burden of protection on piecemeal regulatory guidance rather than mandatory corporate obligations.

The Evidence Act 2011 recognises electronic records and signatures as admissible, while the Cybercrimes Act 2015 criminalises various forms of online fraud and unauthorised access. Both therefore support enforcement in principle. Still, the technical burdens of authentication, certification requirements, and international server locations complicate proof and the provision of swift remedies for aggrieved consumers.

Contribution and scope

This article contributes a focused doctrinal critique of how FCCPA and CAMA interact in the context of electronic contracting, highlighting specific legal uncertainties that affect consumer redress. It proposes concrete statutory clarifications, procedural rules and institutional changes (including recommended FCCPC guidance and CAMA amendments) to make electronic contracting safer for Nigerian consumers. The aim is practical legal reform: to enable courts and regulators to enforce consumer rights effectively in the digital economy.

Conceptual Clarifications

Meaning and Nature of Electronic Contracts

An electronic contract, or e-contract, refers to a contract formed wholly or partly by electronic means, including email, web platforms, mobile apps, or automated systems. The essential features of a contract under Nigerian law, namely offer, acceptance, consideration, intention to create legal relations, and capacity, apply equally in electronic form. The Evidence Act 2011 recognises the admissibility of electronic records and electronic signatures for contractual purposes. This statutory recognition confirms that contracts concluded electronically are not excluded from enforceability in Nigeria.

E-contracts typically manifest as:

1. Clickwrap agreements, where a consumer clicks "I agree" to standard terms before proceeding.
2. Browsewrap agreements, where terms are accessible via a hyperlink and acceptance is inferred from continued use of a website.
3. Shrinkwrap licences, agreements where terms are enclosed with software packaging or revealed during installation.
4. Automated/digital agent contracts, agreements formed through algorithmic systems or smart contracts on blockchain platforms.

While Nigerian courts have not yet issued landmark rulings on the enforceability of clickwrap or browsewrap agreements, comparative case law, such as ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996), shows judicial willingness to uphold such contracts where consent mechanisms are sufficiently clear. Nigerian law, through the Evidence Act 2011 and Cybercrimes Act 2015, accommodates digital signatures and electronic messages as evidence of consent and contract formation.

Consumer Protection Principles

Consumer protection in law aims to correct power and information asymmetries between traders and consumers. In the online environment, these asymmetries are sharper:

- Standard-form contracts drafted unilaterally by businesses.
- Limited bargaining power of individual consumers.
- Technical opacity (algorithmic pricing, automated renewals).
- Cross-border reach of platforms.

The FCCPA 2018 codifies consumer rights to safety, information, choice, and redress. Section 120 prohibits unfair, unreasonable, or unjust contract terms, while section 127 obliges businesses to disclose material information to consumers. However, these provisions are technology-neutral. They apply generally, but do not provide specific rules for electronic transactions. This lack of digital-specific clarity raises doctrinal and enforcement challenges, particularly concerning what constitutes valid consent in an online setting.

Electronic Signatures

Electronic signatures are critical to e-contract validity. Under Nigerian law, the Evidence Act 2011 recognises electronic signatures as functional equivalents of handwritten signatures. The Cybercrimes Act 2015, section 17, further validates electronic signatures where they are reliable and appropriate for the purpose for which the electronic record is generated.

Three types of electronic signatures are often distinguished in comparative practice:

- Simple electronic signatures, e.g., typing a name at the end of an email.
- Advanced electronic signatures, linked uniquely to the signatory and capable of identifying them.
- Qualified electronic signatures, requiring certification by a recognised authority.

Nigeria recognises simple and advanced electronic signatures but lacks a fully developed certification framework comparable to the EU's eIDAS Regulation (Regulation [EU] No. 910/2014). This gap complicates consumer redress in disputes concerning identity fraud or repudiation of consent.

Corporate Legal Personality and Online Conduct

The Companies and Allied Matters Act 2020 (CAMA) modernised Nigerian company law by expressly recognising electronic filings, notices, and general meetings. It also requires companies to maintain transparency and accountability in dealings with the public. Yet CAMA does not specifically regulate consumer-facing electronic contracts. Doctrinally, the corporate veil continues to shield companies from direct liability beyond statutory duties. Hence, enforcement of consumer rights in electronic contracts depends primarily on FCCPA mechanisms rather than CAMA's corporate law framework.

Doctrinal Interface: Contract Law and Consumer Law

The doctrinal interface of contract law and consumer protection law is at the heart of this paper.

- Contract law (offer, acceptance, consideration) ensures enforceability of agreements.
- Consumer law imposes mandatory duties on businesses to protect weaker parties.

In Nigeria, the FCCPA 2018 is the primary consumer law statute, while CAMA 2020 provides the corporate governance context. Together, they shape the legal landscape of electronic contracting. However, the lack of express provisions on online consent, disclosure obligations in digital settings, and remedies for unfair digital practices leaves consumers vulnerable.

Comparative Note on Doctrinal Definitions

Globally, e-contracts are defined broadly:

- The UNCITRAL Model Law on Electronic Commerce (1996) defines data messages and provides that contracts cannot be denied enforceability solely because they are electronic.
- The EU e-Commerce Directive (2000/31/EC) requires Member States to ensure that contracts can be concluded electronically.
- In the UK, the Electronic Communications Act 2000 and case law affirm the enforceability of e-contracts, subject to consumer law protections under the Consumer Rights Act 2015.

Nigeria aligns partially with these standards through the Evidence Act and Cybercrimes Act but lacks the same level of detail in consumer-specific regulation.

The Statutory Landscape

The Federal Competition and Consumer Protection Act (FCCPA) 2018

The FCCPA 2018 is the central statute for consumer protection in Nigeria. It repealed the Consumer Protection Council Act and established the Federal Competition and Consumer Protection Commission as the primary enforcement body. The Act introduces general consumer rights and prohibits unfair, misleading, or exploitative practices. Key provisions include:

- Right to information: Section 114 requires full disclosure of material facts relating to products or services.
- Prohibition of unfair contract terms: Section 120 invalidates contract terms that are unjust, unreasonable or excessively one-sided.
- Obligation to provide notice: Section 127 imposes duties on businesses to disclose relevant information to consumers before transactions.
- Right to redress: Sections 131-133 provide avenues for consumer complaints, remedies and compensation.

While the FCCPA applies across all sectors, it was not designed specifically with electronic contracting in mind. Its provisions are technology-neutral, leaving uncertainty on critical digital issues. Does clicking "I agree" constitute sufficient consent under section 120?

- Are hidden "browsewrap" terms enforceable if the consumer is not given adequate notice of them?

Companies and Allied Matters Act (CAMA) 2020

The CAMA 2020 modernises Nigerian company law and significantly integrates digital processes into corporate governance and administration. Key innovations relevant to online commerce include:

- Electronic filings: Section 176 permits electronic filing, electronic share transfer and electronic maintenance of company records.
- Virtual meetings: Section 240 allows private companies to hold general meetings electronically.
- Electronic notices: Companies may now issue notices via email or other electronic means.

These provisions confirm legislative recognition of digital corporate processes. However, CAMA does not explicitly regulate how companies must conduct consumer-facing online transactions. Its consumer-protection implications are indirect:

- Directors' duties (Part IX) require companies to act in the best interests of the company, which may arguably extend to fair online dealings.
- Corporate liability under CAMA may arise where a company engages in fraudulent or misleading conduct online.
- The Corporate Affairs Commission (CAC), as registrar, enforces compliance with filing obligations but does not directly handle consumer complaints.

Thus, while CAMA 2020 fosters digital corporate accountability, it does not create explicit rules to protect consumers in electronic contracting. Enforcement remains largely under the FCCPA.

Evidence Act 2011

The Evidence Act 2011 provides the doctrinal basis for recognising electronic records and electronic signatures in Nigeria. Key provisions include:

- Section 84: Admits electronic records as evidence if properly certified.
- Section 93: Recognises that a contract may be formed or evidenced electronically.
- Section 258: Defines "document" to include electronic records.

These provisions are crucial in disputes over electronic contracts. For example, where a consumer claims not to have consented to online terms, electronic logs, email correspondence, or digital acceptance records may be admissible.

Challenges remain because the certification requirement for electronic evidence under section 84 can be technically demanding, particularly where servers are located outside Nigeria. Authentication of electronic signatures is also not always straightforward in practice, as Nigeria lacks a fully developed public key infrastructure or certification authority system comparable to the EU's eIDAS Regulation. Thus, while the Evidence Act lays a foundation, procedural hurdles complicate effective consumer enforcement in e-contract disputes.

Cybercrimes (Prohibition, Prevention, etc.) Act 2015

The Cybercrimes Act 2015 criminalises various forms of online misconduct, including identity theft, phishing, and electronic fraud. Section 17 validates electronic signatures, making them legally binding. Section 18 criminalises identity theft and impersonation, which often occur in online transactions. From a consumer-protection perspective, the Cybercrimes Act addresses the criminal dimension of e-commerce disputes. For instance, if an online trader uses false identities or engages in cyber fraud, consumers may seek redress through criminal prosecution. However, enforcement depends heavily on technical capacity and inter-agency cooperation among the police, EFCC, and FCCPC. The limitation is that the Act is not consumer-centred: its focus is national cybersecurity rather than consumer redress. Consumers harmed by online fraud often find themselves navigating multiple institutions without clarity about jurisdiction.

NITDA Guidelines and Regulatory Instruments

The National Information Technology Development Agency (NITDA) issues regulations and guidelines that affect e-contracting indirectly, particularly in areas of data protection and ICT governance. The Nigeria Data Protection Regulation (NDPR) 2019, issued by NITDA, was Nigeria's first comprehensive framework on data privacy in digital transactions. It has now been superseded by the Nigeria Data Protection Act (NDPA) 2023, which established the Nigeria Data Protection Commission (NDPC). While NITDA's earlier role was transitional, its guidelines shaped the early governance of online business practices, particularly concerning consumer data and consent.

Nigeria Data Protection Act (NDPA) 2023

The NDPA 2023 creates a comprehensive statutory framework for data protection, privacy, and processing. It establishes the Nigeria Data Protection Commission (NDPC) and introduces duties for data controllers and processors. For electronic contracts, consumer data is central because personal information is processed for registration, payments, deliveries, and profiling. The NDPA therefore strengthens consumer protection by:

- Requiring lawful basis for processing (consent, contract, legal obligation).
- Mandating data minimisation and purpose limitation.
- Imposing security obligations on businesses.
- Granting consumers rights of access, correction, and deletion.

Although not strictly a contract law statute, the NDPA fills an important consumer-rights gap in e-commerce. Without robust privacy protections, contractual consent may be undermined by information asymmetry and misuse of personal data.

Doctrinal Synthesis

Taken together, these statutes create a fragmented but interlinked framework for electronic contracts and consumer protection:

- FCCPA 2018: consumer rights and enforcement.
- CAMA 2020: corporate governance in a digital era.
- Evidence Act 2011: recognition of electronic evidence and signatures.
- Cybercrimes Act 2015: criminalisation of online fraud.
- NDPA 2023: data protection and privacy rights.

The doctrinal problem is that no single statute integrates these frameworks for online commerce. Instead, consumer protection in electronic contracts requires navigating multiple overlapping laws and institutions. This creates legal uncertainty and undermines effective redress.

Doctrinal Analysis of FCCPA and CAMA in Electronic Contracting

FCCPA 2018: Consumer Protection in the Digital Marketplace

The FCCPA 2018 is the first statute in Nigeria to consolidate consumer protection and competition regulation. Doctrinally, its provisions extend to contracts and commercial transactions generally, including electronic contracts. Yet the Act's silence on the unique features of e-commerce raises practical and interpretive problems.

Right to Information

Section 114 of the FCCPA requires suppliers to disclose material facts about goods and services. In the context of electronic contracts, this principle means that online traders must present clear, accessible terms before consumers give consent. The problem is that online platforms often bury key terms in hyperlinks or lengthy standard-form contracts. This risks breaching the FCCPA's transparency mandate. By comparison, the EU Consumer Rights Directive 2011/83/EU requires traders to provide pre-contractual information in a “clear and comprehensible manner”. Nigerian law lacks this specificity, which provides a useful lesson for reform.

Prohibition of Unfair Contract Terms

Section 120 invalidates contract terms that are excessively one-sided. In e-contracts, standard terms are usually non-negotiable. A “click” or “tap” by the consumer constitutes consent, but the fairness of the underlying terms remains questionable. A doctrinal gap therefore arises because the FCCPA does not specify when clickwrap or browsewrap contracts are considered unfair. Nigerian courts have also not yet developed case law on digital adhesion contracts comparable to US courts, for example, Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002), in which browsewrap terms that were not clearly disclosed were not enforced.

Right to Redress

Sections 131-133 empower consumers to seek remedies through the FCCPC. This theoretically extends to online disputes. However, the FCCPC lacks a dedicated online dispute resolution (ODR) mechanism for electronic contracts. Remedies may require in-person complaints, making enforcement inaccessible to many digital consumers. Administrative sanctions, including fines and orders, exist, but consumer compensation in online fraud cases is weakly enforced.

Enforcement and Jurisdictional Gaps

A major doctrinal issue is whether FCCPA rights apply to foreign-based online platforms (e.g., Amazon, Alibaba, or social media marketplaces). The Act is territorially bound, and enforcement against non-resident companies is limited without cross-border agreements.

CAMA 2020: Corporate Governance and Digital Accountability

The CAMA 2020 was hailed as Nigeria's most ambitious corporate law reform in decades. It introduced electronic governance mechanisms but remains limited in addressing consumer protection directly.

Electronic Filing and Notices

By recognising electronic filings (section 176) and electronic general meetings (section 240), CAMA acknowledges the legitimacy of digital corporate practices. This indirectly supports the legitimacy of corporate electronic contracting. Its doctrinal strengths include alignment with international norms and encouragement of online commerce. However, there is no explicit requirement that companies conducting online consumer transactions comply with enhanced disclosure or fairness obligations.

Directors' Duties and Consumer Interests

CAMA places fiduciary duties on directors (Part IX). Nigerian law traditionally frames these duties towards the company and its shareholders, rather than directly towards consumers. Doctrinally, one could argue that systemic consumer protection forms part of the "best interests of the company", since consumer trust sustains corporate reputation. However, absent explicit statutory wording, courts may resist extending directors' duties to consumer-facing obligations.

Corporate Liability in Digital Misconduct

Companies may face liability under CAMA if they engage in fraud or misrepresentation. For example, online businesses that conceal terms, engage in pyramid schemes, or issue false electronic advertisements could fall within CAMA's fraudulent trading provisions. The challenge is that enforcement depends on proactive action by the Corporate Affairs Commission (CAC), which focuses mainly on corporate filings rather than consumer protection. This creates institutional fragmentation. CAC enforces CAMA, while the FCCPC enforces FCCPA, leaving gaps where digital corporate misconduct harms consumers.

The FCCPA-CAMA Interface: Fragmented Doctrinal Protection

Doctrinally, FCCPA and CAMA operate in parallel rather than in harmony. FCCPA governs consumer rights in commercial transactions, while CAMA governs corporate governance and business operations. Issues arising from this separation include the absence of direct cross-reference: CAMA does not mandate compliance with consumer protection norms under the FCCPA. There is therefore overlapping jurisdiction. FCCPC and CAC may both handle misconduct by online companies, but there is no statutory mechanism for cooperation. There is also limited judicial guidance. Nigerian courts have not yet clarified how consumer protection claims under the FCCPA should interact with corporate obligations under CAMA in digital transactions. Comparatively, in jurisdictions such as the UK, the Consumer Rights Act 2015 and the Companies Act 2006 operate more synergistically: directors' duties explicitly consider broader stakeholder interests, while consumer law provides strong digital protections. Nigeria's fragmented regime falls short of this coherence.

Doctrinal Consequences for Electronic Contracts

From the doctrinal analysis of FCCPA and CAMA, the following consequences emerge:

1. Uncertainty on consent: No explicit statutory recognition of clickwrap/browsewrap consent models, leaving ambiguity.
2. Weak corporate accountability: Directors' duties under CAMA do not expressly cover consumer-facing online practices.
3. Fragmented enforcement: FCCPC and CAC operate separately, leading to regulatory gaps.
4. Limited digital dispute mechanisms: FCCPC lacks ODR processes tailored for electronic contracts.
5. Risk of forum shopping: Consumers harmed by online companies may struggle to identify the appropriate regulator or court.

Evidence, Enforcement and Remedies in Electronic Contracting

Evidentiary Framework in Electronic Contracts

One of the main challenges of consumer protection in online transactions lies in proving contract formation, consent, and breach. Electronic evidence in Nigerian law is governed by the Evidence Act 2011 (as amended), which recognises electronic records and digital signatures as admissible, provided that applicable reliability requirements are met. This doctrinal recognition allows online contracts, including clickwrap, browsewrap, and electronic signatures, to be enforced in Nigerian courts. However, challenges remain because courts may lack technical expertise in evaluating digital evidence, such as metadata, encryption, or blockchain records. Consumers also rarely have the resources to retrieve reliable electronic evidence when disputes arise.

Burden of Proof in E-Commerce Disputes

Traditionally, Nigerian contract law follows the common law principle that the party asserting must prove. This creates hurdles for consumers in online cases, where companies typically control the data. Comparatively, in the EU, the Consumer Rights Directive shifts the burden onto suppliers to prove that they complied with information and consent requirements. Nigeria has yet to adopt such consumer-friendly presumptions.

Enforcement Institutions

The Federal Competition and Consumer Protection Commission is the main enforcement body under the FCCPA. Its powers include issuing compliance directives, investigating consumer complaints, imposing administrative fines, and instituting actions in court. However, it faces weaknesses. The FCCPC has no specialised digital commerce unit, and consumer complaint processes can be slow and inaccessible to those harmed in fast-moving online transactions. Enforcement against cross-border digital businesses remains practically difficult without appropriate international arrangements.

The Corporate Affairs Commission (CAC) enforces CAMA, ensuring corporate accountability. While it can sanction companies for fraudulent practices, its mandate is not consumer-facing. This creates a regulatory overlap with the FCCPC. For example: An online company misrepresenting its services could face FCCPC action for unfair practices, while CAC could simultaneously sanction it for corporate misconduct, yet no coordination mechanism exists.

Judicial enforcement happens with the Nigerian courts retaining jurisdiction over contractual disputes. However, courts are often slow and expensive, making them unsuitable for consumer-level disputes. Judges may apply traditional contract doctrines without fully accounting for the realities of electronic adhesion contracts. In practice, many consumers do not litigate small-value online disputes, leading to systemic under-enforcement.

Remedies Available to Consumers

These include statutory remedies under the FCCPA, judicial remedies, Alternative Dispute Resolution (ADR), and ODR. Statutory remedies under the FCCPA may enable consumers to obtain compensation for harm caused by defective goods or services (section 131), rescission of unfair contracts (section 120), and administrative redress through FCCPC directives. However, enforcement of compensation provisions is weak. Many outcomes involve fines against companies rather than direct consumer redress.

Judicial and contractual remedies, including damages, rescission, and injunctions, are theoretically available. However, barriers include the high cost of litigation relative to the value of most online transactions, the technical complexity of proving breach in digital environments, and delays in adjudication. While there are avenues for limited Alternative Dispute Resolution (ADR), there is no institutionalised ODR platform for Nigerian consumers. The Arbitration and Mediation Act 2023 supports electronic arbitration and mediation. While this creates opportunities for ODR in consumer disputes, it remains largely confined to commercial disputes among businesses (B2B) rather than business-to-consumer (B2C) disputes. There is no institutionalised ODR platform for Nigerian consumers comparable to the EU's ODR Portal under Regulation 524/2013. Private initiatives, such as online platforms offering internal complaint resolution, exist but lack neutrality or statutory legitimacy.

Cross-Border Enforcement Challenges

E-commerce is inherently transnational. Nigerian consumers frequently transact with companies based abroad, including Amazon, Alibaba, Shein, and Temu. This creates significant challenges involving jurisdictional limitations, conflict of laws, and enforcement gaps. Nigerian courts lack practical reach over non-resident companies. Contracts often include foreign choice-of-law clauses, which may disadvantage Nigerian consumers. Even if a Nigerian consumer wins a case, enforcing judgments abroad is difficult without reciprocal arrangements. Comparatively, the EU ensures cross-border consumer enforcement through coordinated mechanisms such as the Consumer Protection Cooperation (CPC) Regulation 2017/2394. Nigeria lacks comparable integration, either regionally within ECOWAS or globally.

Doctrinal Implications

Several doctrinal implications arise. The first concerns the relationship between admissibility and accessibility. Others include institutional fragmentation, weak remedies, underutilisation of ADR and ODR, and the cross-border enforcement gap. While the Evidence Act admits electronic records, consumers face barriers in gathering and presenting such evidence. FCCPC and CAC operate in silos, leading to overlapping or inconsistent enforcement. Statutory remedies exist but are rarely realised in practice because of weak enforcement mechanisms. ADR and ODR are underutilised. The Arbitration and Mediation Act 2023 opens opportunities, but there is no consumer-facing infrastructure. Nigerian law also lacks regional or international frameworks to protect digital consumers transacting across borders.

ODR in Comparative Perspective

This section synthesises comparative experience with Online Dispute Resolution (ODR) to draw doctrinal lessons for Nigeria. It concentrates on five jurisdictions or sets of instruments that have materially shaped ODR design: the European Union, with its regulatory approach and electronic-signature regime; UNCITRAL, with its technical guidance; the United States, with its institutional practice and agency guidance; selected Asian models, including Singapore, India, and China; and African experiments, including Kenya, South Africa, and regional initiatives. For each, the discussion sets out core design features, doctrinal innovations, and practical strengths and weaknesses, and then derives targeted lessons for Nigerian law reform and institutional design.

European Union

The EU's regulatory architecture, ODR intake, and electronic-signature law provide two complementary lessons for Nigeria. First, the EU's Regulation on ODR for consumer disputes (Regulation 524/2013) created a central ODR Portal to provide multilingual intake and triage for cross-border consumer complaints. The portal was designed as a neutral gateway that referred cases to accredited ADR bodies rather than deciding disputes itself. This centralised intake and distributed resolution model reduced search costs for consumers and made cross-border complaints more visible to regulators and policy-makers. Second, the EU's legal regime for electronic signatures, consolidated under the eIDAS Regulation 910/2014, supplies doctrinal certainty by categorising electronic signatures as simple, advanced, or qualified, and by ensuring that an electronic signature cannot be denied legal effect solely because it is electronic. eIDAS therefore removes formal objections to digitally signed awards, electronically concluded contracts, and online consent mechanisms, while coupling formal recognition with a trust-service infrastructure for authentication and cross-border recognition.

Second, the EU’s legal regime for electronic signatures (now consolidated under eIDAS Regulation 910/2014) supplies doctrinal certainty by categorising electronic signatures (simple, advanced, qualified) and by ensuring that an electronic signature cannot be denied legal effect solely because it is electronic. eIDAS therefore removes formal objections to digitally signed awards, electronically-concluded contracts, and online consent mechanisms, while coupling this formal recognition with a trust-service infrastructure for authentication and cross-border recognition. This combination of an intake/regulatory portal and a rigorous e-signature trust framework is powerful: intake and enforceability are both addressed. Recent developments also show the EU reassessing the effectiveness of its ODR Portal. Usage has been uneven, prompting policy reappraisal of centralised ODR and the appropriate role of mandatory platform links for traders. The practical lesson is that visibility alone does not guarantee dispute resolution. Conversion of complaints into settlements requires accredited providers, incentives, and user trust. A central intake gateway, whether public or public-private, improves visibility and access, but must be paired with trustworthy accreditation and measurable conversion processes. A clear legal regime on electronic signatures, combining recognition with trust services, reduces enforceability friction for electronically concluded contracts and online awards.

UNCITRAL, principled, technology-neutral guidance

UNCITRAL's Technical Notes on ODR (2016) are the principal international, non-binding instrument aimed at assisting States, especially developing States, to design ODR systems that are fair, accessible, and interoperable. UNCITRAL frames ODR as a systems-design problem, emphasising triage, transparency, impartiality, data protection by design, accessibility for low-bandwidth users, and mechanisms for cross-border interoperability. The Notes caution against over-reliance on automation without human oversight and stress due-process protections for algorithmic decision-support. UNCITRAL's guidance is doctrinally neutral in that it does not impose one institutional model on States, but it is normative in insisting that ODR preserve procedural fairness, avoid exclusion, and provide transparent appeal and escalation channels. For Nigeria, a jurisdiction with heterogeneous connectivity and strong consumer-protection needs, UNCITRAL offers an adaptable blueprint that prioritises access and safeguards over technological determinism. Key doctrinal lessons for Nigeria include the adoption of a tiered ODR architecture, comprising automated negotiation, assisted mediation, and human adjudication, with explicit escalation and appeal routes. Data-protection and accessibility requirements should also be embedded into platform design, including privacy by design and low-bandwidth modes.

United States' institutional rules, agency guidance and marketplace regulation

The United States lacks a single federal ODR statute, but has extensive institutional and agency practice. Leading arbitral institutions, such as AAA/ICDR, and courts have issued model rules and virtual-hearing orders that operationalise online procedure through technical pre-hearing checks, secure testimony protocols, evidentiary authentication practices, and contingency plans for connectivity failures. Agencies such as the Federal Trade Commission have issued guidance on online marketplaces and consumer protection. Recent federal legislative efforts, including the INFORM Act and Online Consumer Protection proposals, also reflect an emphasis on platform accountability and marketplace transparency. The doctrinal strength of the US institutional approach is that party autonomy, combined with robust institutional rules, can validate ODR rapidly even in the absence of new primary legislation. Procedural model orders reduce uncertainty and build practitioner confidence. However, this approach depends on well-resourced institutions and active agency oversight. Institutional bodies, including local arbitral centres and the FCCPC, can promulgate model ODR procedures immediately to provide legal certainty while legislative reform proceeds. Agency regulation of marketplace intermediaries can complement ODR by reducing harm upstream, including fraud and misrepresentation. Asian jurisdictions also provide several practical designs. Singapore combines a pro-arbitration legal environment with institutional excellence, including SIAC and SIMC, and strong digital court initiatives. India has produced policy roadmaps that favour phased roll-out, stakeholder capacity building, and sectoral pilots. China demonstrates the scalability of government-led consumer complaint platforms, which can handle high volumes but raise questions of independence and due process.

Countries that pair legal certainty, institutional capacity, and gradual implementation tend to achieve better adoption and trust. Government-led platforms can scale, but must ensure procedural impartiality to gain commercial credibility. For Nigeria, the lesson is to consider a phased, sectoral pilot approach, particularly in e-commerce and fintech, to test ODR design before national roll-out, and to establish trusted and accredited centres as an institutional investment. This is as important as the technology itself in delivering effective outcomes.

Across Africa, ODR and digital consumer-protection initiatives are emerging unevenly. Kenya has developed ADR and data-dispute frameworks and has engaged in ODR pilots. Its Data Protection Act 2019 and ODPC guidance intersect with dispute-resolution design. South Africa has debated e-dispute systems for consumers and strengthened data-protection enforcement under POPIA. Regional instruments, including the AU Malabo Convention and ECOWAS initiatives, point to a future need for interoperability of ODR across African markets. African jurisdictions often confront the same obstacles as Nigeria, including infrastructure gaps, digital literacy challenges, and limited institutional resources. They also share policy space for regional cooperation through ECOWAS and AfCFTA, which can amplify interoperability and enforcement. Early evidence suggests that pilots and targeted sectoral programmes are realistic routes forward. Nigeria should give priority to regional interoperability through ECOWAS and AfCFTA to address cross-border e-commerce disputes. National data-protection institutions should also be considered in establishing privacy and security standards for ODR providers.

Institutional and Enforcement Implications for Electronic Contracts in Nigeria

Institutional Fragmentation and Overlap

Nigeria's consumer-protection and corporate-governance landscape involves multiple institutions with overlapping mandates. These include the Federal Competition and Consumer Protection Commission, which is empowered under the FCCPA to regulate consumer rights, investigate complaints, and enforce penalties; the Corporate Affairs Commission (CAC), which serves as a corporate regulator under CAMA, supervising company registration, governance, and disclosure; the Nigeria Data Protection Commission (NDPC), which regulates data protection under the NDPA 2023; and the judiciary, which interprets and enforces rights and obligations under contract and consumer law. The problem is that these institutions lack a coordinated framework for electronic contracting and consumer disputes. For instance, while the FCCPC has broad consumer jurisdiction, many online businesses fall under CAC oversight, and consumer complaints involving personal data implicate the NDPC. Without coordination, consumers face a fragmented enforcement ecosystem. This fragmentation dilutes accountability. A more integrated model, akin to the EU's CPC Network, could strengthen cross-agency enforcement for digital markets.

Enforcement Challenges in Electronic Contracting

Nigerian courts remain inaccessible to many consumers because of cost and delay. The FCCPC offers administrative redress, but this can be bureaucratic and lacks nationwide coverage. The absence of a dedicated Online Dispute Resolution (ODR) system for consumers means that many disputes remain unresolved. Under Nigerian law, the consumer bears the burden of proving consent, terms, or breach of contract. In digital contexts, businesses typically control the relevant data, including server logs and transaction metadata. This places consumers at a structural disadvantage. By contrast, in the EU, the Consumer Rights Directive places obligations on suppliers to prove compliance, reversing the burden of proof in many cases. Nigeria could adopt similar statutory presumptions.

Most Nigerian consumers transact with foreign e-commerce platforms. The FCCPC and Nigerian courts lack effective jurisdiction over foreign companies absent reciprocal treaties. As a result, Nigerian consumers remain vulnerable in cross-border e-commerce. Although the FCCPA provides remedies, including rescission, damages, and restitution, enforcement is often limited to administrative fines imposed on companies, with little direct restitution to consumers.

Applying insights from comparative perspectives shows that Nigeria could establish a National Consumer ODR Portal, coordinated by the FCCPC, to triage online complaints and connect them with accredited ODR providers, drawing on the EU's central intake portal. Nigeria could also adopt a multi-tier ODR system comprising negotiation, mediation, and adjudication, with digital escalation pathways, drawing on the UNCITRAL model. Following the US approach, the FCCPC and arbitral institutions could develop Model Rules for Online Hearings and digital evidence to give practitioners greater certainty. Drawing on Asian experience with phased pilots, Nigeria could begin with sector-specific pilots in e-commerce and fintech before rolling out ODR nationwide. Collaboration with ECOWAS and AfCFTA is also critical to enforcing consumer rights in cross-border digital transactions.

FCCPA 2018 should be amended to explicitly recognise electronic contracts, shift the burden of proof to businesses in specified digital disputes, and mandate ODR as a first-tier redress mechanism for online consumers. CAMA 2020 could be harmonised with the FCCPA by requiring companies engaged in e-commerce to designate digital compliance officers responsible for consumer complaints and ODR participation. The Evidence Act 2011 should be updated with rules for metadata, blockchain records, and smart contracts to support the admissibility of emerging forms of digital evidence. The Arbitration and Mediation Act 2023 provides a doctrinal foundation for ODR but requires consumer-specific rules. The NDPA 2023 ensures data privacy in digital contracting, but its enforcement could be linked more closely to consumer protection. For example, data breaches in e-commerce could trigger joint investigations by the FCCPC and NDPC.

FCCPA 2018 should be amended to explicitly recognise electronic contracts, shift the burden of proof to businesses in digital disputes, and mandate ODR as a first-tier redress mechanism for online consumers. CAMA 2020 could be harmonised with FCCPA by requiring companies engaging in e-commerce to register digital compliance officers responsible for consumer complaints and ODR participation. Evidence Act 2011 should be updated with rules for metadata, blockchain records, and smart contracts to support admissibility of emerging forms of digital evidence. Arbitration and Mediation Act 2023 provides a doctrinal foundation for ODR but requires consumer-specific rules. NDPA 2023 ensures data privacy in digital contracting, but its enforcement should be linked to consumer protection, for example, data breaches in e-commerce should trigger FCCPC and NDPC joint investigations.

Contract formation requires offer and acceptance accompanied by a sufficiently clear manifestation of consent. Electronic contracting challenges traditional assumptions about meaningful assent. Clickwrap mechanisms, involving explicit “I agree” clicks, are usually defensible as evidence of assent, whereas browsewrap mechanisms, in which terms are accessible only through a hyperlink, are weaker. The Evidence Act 2011 admits electronic records and signatures, but remains neutral on the quality of consent or the standard for electronic notice.

The FCCPA's transparency obligations require disclosure of "material facts", yet the statute does not articulate specific standards for digital presentation. It does not specify what constitutes "clear and comprehensible" pre-contract information in low-attention online environments. Consequently, businesses can comply in form by providing a link, while failing in substance by burying key clauses. This gap mirrors critiques in other jurisdictions where formal recognition of electronic signatures produced compliance in form without effective consumer protection.

Remedial doctrinal stance: adopt a presumption that, in B2C electronic contexts, suppliers bear the burden of demonstrating that notice was provided in a reasonably visible and intelligible manner and that the consumer had a fair opportunity to review key contractual terms before assent. FCCPA rules or subsidiary regulations should specify minimum design standards for online notices, including font size, explicit callouts for key clauses, and prohibition of pre-ticked boxes.

Contract formation requires offer and acceptance accompanied by a sufficiently clear manifestation of consent. Electronic contracting challenges traditional assumptions about "meaningful" assent. Clickwrap mechanisms (explicit "I agree" clicks) are usually defensible as evidence of assent; browsewrap mechanisms (terms accessible only by hyperlink) are much weaker. The Evidence Act 2011 admits electronic records and signatures (s.84, s.93), but the Act is neutral on the quality of consent or the standard for electronic notice.

Standard-form online contracts are paradigmatic adhesion contracts. Consumers face take-it-or-leave-it terms that can include exclusion clauses, automatic renewals, or arbitration clauses that limit remedies. Section 120 of the FCCPA invalidates "unfair" terms but does not define clear tests for digital adhesion contexts. Nigerian courts have yet to develop a robust unconscionability doctrine adapted to digital markets. Without doctrinal indicators such as relative bargaining power, notice, opt-out possibilities, and reasonableness review, judicial scrutiny of online terms may be inconsistent. In practice, this leaves consumers vulnerable to "dark patterns", design techniques that manipulate consent, which the FCCPA does not expressly target.

Nigeria's current enforcement architecture under the FCCPA 2018 and CAMA 2020 is doctrinally sound in principle but weak in practice. Consumers face barriers of cost, evidence, and jurisdiction that make remedies illusory. Comparative experience shows that doctrinal reforms, such as burden-of-proof shifts, recognition of electronic signatures, and structured ODR frameworks, together with institutional reforms, including central intake, coordinated enforcement, and regional interoperability, can transform consumer protection in electronic contracting. Without these reforms, Nigerian consumers remain vulnerable in the rapidly expanding digital marketplace. With them, Nigeria could align with international best practice and lead within Africa in building a fair and trustworthy e-commerce ecosystem.

Algorithmic Contracting and the Transparency Imperative

Automated contracting, algorithmic profiling and dynamic pricing complicate traditional doctrines. Algorithms can determine price, eligibility, or even whether a contract is offered, decisions that affect consumer choice and equality of treatment. The NDPA 2023 introduces data-subject rights that are relevant here (access, rectification, portability), but it does not by itself solve deep transparency questions about algorithmic logic. Electronic contracts routinely involve non-resident suppliers. FCCPA enforcement is territorially constrained, while CAMA governs corporate actors registered in Nigeria but is silent on extraterritorial platforms. Judicial enforcement of Nigerian judgements or FCCPC orders against foreign entities is practically difficult. The absence of clear rules on choice of law, forum selection in consumer contexts, and mutual enforcement treaties creates a situation in which consumers may be unable to secure remedies against foreign suppliers. Although the Evidence Act accommodates electronic evidence, practical doctrinal problems persist: (a) consumers rarely have access to server logs or metadata that prove assent; (b) certification requirements (s.84) can be technical and costly; (c) cross-border hosting complicates chain-of-custody and authentication.

The evidentiary asymmetry tilts litigation in favour of suppliers, who typically control logs and transactional records. Courts unfamiliar with digital forensics may undervalue consumer-side evidence. A remedial doctrinal stance is to create a statutory Digital Markets Coordination Mechanism, whether a task force or memorandum of understanding, that harmonises enforcement, shares data, and provides a single public ODR intake portal. The FCCPC should be empowered, statutorily or administratively, to act as the consumer-facing integrator, with the NDPC handling privacy aspects and the CAC supervising corporate sanctions, supported by fast-track inter-agency procedures for joint investigations and direct consumer restitution.

Enforcement, Jurisdiction and the Cross-Border Problem

Doctrinal protections are meaningless if significant segments of the population cannot access or effectively use digital dispute systems. Nigeria's digital divide, reflected in uneven broadband, limited device ownership, and low digital literacy in rural areas, means that many consumers will be disadvantaged by an online-first regulatory approach. Reliance on e-processes risks excluding the poorest and least digitally literate, contrary to access-to-justice norms. A remedial doctrinal stance should therefore enforce a hybrid model, with online channels complemented by assisted access points, such as community legal centres, kiosks, and mobile outreach, together with low-bandwidth, mobile-first design of any ODR mechanism. Pro-consumer presumptions concerning notice and burden of proof should be especially protective where consumers face demonstrable access constraints.

From the critiques above, several doctrinal principles emerge: substance over form, where legal recognition of electronic signatures and electronic records must be paired with substantive standards for notice and meaningful consent; consumer-favouring presumptions, whereby B2C online contexts impose evidential and disclosure duties on suppliers; algorithmic accountability, which treats automated decision-making as attributable corporate conduct and requires explainability and appeal rights; coordinated enforcement, which creates statutory mechanisms for inter-agency cooperation and a central consumer intake and ODR facility; and inclusive design, which ensures hybrid access modes and protections for digitally excluded populations. These doctrinal reforms require legislative amendments to the FCCPA and targeted rule-making by the FCCPC, CAC, and NDPC. They also demand judicial willingness to interpret existing statutes purposively in favour of consumer protection in the digital environment.

Doctrinal reform must not pit innovation against protection. Well-designed rules can preserve party autonomy and commercial efficiency while ensuring that consent is genuine, processes are transparent, and remedies are realistic. Nigeria's present statutes, including the FCCPA 2018, CAMA 2020, Evidence Act 2011, and NDPA 2023, provide building blocks. Without doctrinal recalibration focused on the digital realities identified above, however, consumers will continue to face structural disadvantages in electronic contracting.

Conclusion

Electronic contracting has become the backbone of modern commerce in Nigeria, from online retail and financial services to telecommunications and digital platforms. The FCCPA 2018 and CAMA 2020 mark important milestones in aligning Nigerian law with global best practices in consumer protection and corporate governance. Yet, as this paper has shown, doctrinal and institutional weaknesses remain significant. At the level of consent and disclosure, Nigerian law has not yet provided detailed statutory guidance on what constitutes valid consumer assent in digital environments. The rise of clickwrap, browsewrap, and automated contracts demonstrates the urgent need for clear, consumer-friendly presumptions. Without these, courts are left to improvise, with results that may lack coherence and predictability.

At the level of evidence and proof, consumers face a daunting asymmetry of information. While the Evidence Act 2011 recognises electronic records, in practice the evidentiary burden rests heavily on consumers who lack access to key transactional data controlled by suppliers. Doctrinal reform is needed to rebalance this burden, coupled with judicial capacity building in digital forensics. At the level of corporate accountability, the gap between CAMA 2020's governance reforms and consumer protection duties is stark. Directors' obligations remain primarily inward-looking, towards shareholders, rather than outward-looking towards consumers. A doctrinal shift to embed consumer rights within corporate governance would reinforce accountability and align Nigeria with international standards of responsible digital commerce. At the level of cross-border enforcement, the territorial limits of Nigerian law collide with the borderless nature of the digital economy. Without strong international cooperation frameworks, Nigerian consumers remain vulnerable when contracting with foreign suppliers. Comparative experience from the EU, UNCITRAL, and regional ODR mechanisms offers concrete models for Nigeria to adapt.

Finally, access and inclusion remain persistent challenges. Legal protections cannot be meaningful if consumers lack the digital literacy, infrastructural access, or institutional support to exercise their rights. The digital divide risks transforming e-contracts into another layer of exclusion rather than empowerment. Nigeria stands at a crossroads. On one path lies a fragmented, under-enforced regime that leaves consumers exposed and undermines confidence in e-commerce. On the other lies a forward-looking, harmonised regime that not only protects consumers but also positions Nigeria as a digital leader in Africa. The choice requires political will, legislative clarity, regulatory coordination, and institutional investment. Thus, the future of electronic contracts and consumer protection in Nigeria depends on doctrinal precision and institutional innovation. If Nigeria can translate its statutory reforms into coherent, enforceable protections tailored for the digital age, it will foster consumer trust, attract investment, and consolidate its role as a hub for Africa's digital economy.

Recommendations for Institutional Reform

The doctrinal and institutional reforms proposed in this paper offer a road-map for a consumer-centred digital economy. They include clarifying digital consent, rebalancing evidentiary burdens, extending corporate duties, strengthening cross-border frameworks, and embedding ODR infrastructure. The FCCPA, CAMA, Evidence Act, Cybercrimes Act, and NDPA must be read and reformed as an integrated framework, not as siloed statutes. This paper recommends the following:

1. Inter-Agency Coordination: Establish a Digital Markets Taskforce (FCCPC, CAC, NDPC, Judiciary) to coordinate enforcement of electronic contracts.
2. Legislative Reform: Amend FCCPA to incorporate explicit e-commerce and ODR provisions, including presumptions in favour of consumers.

3. ODR Infrastructure: Launch a Consumer ODR Portal integrated with FCCPC complaint mechanisms, following the EU intake model.
4. Sectoral Pilots: Begin ODR pilots in fintech (digital lending, mobile payments) and e-commerce (marketplaces, logistics).
5. Regional Cooperation: Advocate for an ECOWAS ODR Protocol to enable enforcement of consumer awards across West Africa.
6. Judicial Training: Provide training for judges on digital evidence, electronic signatures, and consumer protection principles.
7. Consumer Awareness: Public campaigns on consumer rights in e-commerce, including digital literacy and privacy awareness.

References

Ajayi, O. (2020). Corporate governance reforms under CAMA 2020: Implications for Nigerian businesses. *Nigerian Business Law Review, 8(1)*, 12-34.

Ajibola, T. (2022). Consumer protection in Nigeria's e-commerce sector: A doctrinal appraisal of the FCCPA 2018. *African Journal of Commercial Law, 5(3)*, 77-99.

Akeredolu, D. (2020). Online contracts and consumer protection in Nigeria: An analysis of the FCCPA 2018. *Nigerian Law Journal, 24(1)*, 101-124.

Amanze, C. (2021). The digital divide and consumer access to justice in Nigeria. *Journal of Consumer Policy in Africa, 9(2)*, 201-225.

Bamodu, G. (2022). Nigerian corporate law and consumer rights: Reconciling conflicts under CAMA 2020. *African Commercial Law Review, 14(1)*, 56-80.

Benson, R. (2020). Globalisation and cross-border consumer protection: Lessons for Nigeria. *Journal of International Trade Law and Policy, 19(4)*, 301-320.

Brownsword, R. (2019). Law, technology and society: Re-imagining regulation for the digital age. Routledge.

Chukwuma, P. (2022). Evidence in electronic commerce disputes under Nigerian law. *Nigerian Evidence Law Review, 11(2)*, 49-73.

Companies and Allied Matters Act, CAMA. (2020).

Cybercrimes (Prohibition, Prevention, etc.) Act. (2015). https://placng.org/i/wp-content/uploads/2019/12/Federal-Competition-and-Consumer-Protection-Act-2018.pdf

Data Protection Office. (n.d.). ADR framework and guideline. https://www.odpc.go.ke/wp-content/uploads/2024/02/ADR-FRAMEWORK-amp-GUIDELINE.pdf

Ekanem, E. O. (2016). Online contracts in Nigeria: An overview. University of Nigeria, Nsukka. https://law.unn.edu.ng/wp-content/uploads/sites/12/2016/08/Article-4-Online-Contracts-in-Nigeria_An-Overview-Edwin-O.-Ezike.pdf

EUR-Lex. (n.d.). Solving consumer-trader disputes arising from online shopping. https://eur-lex.europa.eu/EN/legal-content/summary/solving-consumer-trader-disputes-arising-from-online-shopping.html

European Commission. (n.d.). What is the legislation? eSignature. https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109076/What%2Bis%2Bthe%2Blegislation%2B-%2BeSignature

European Union. (2019). Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services. Official Journal of the European Union, L136.

Federal Competition and Consumer Protection Commission. (2021). Guidelines on digital lending practices in Nigeria. Abuja, Nigeria: FCCPC.

Federal Competition and Consumer Protection Commission. (2022). Limited interim regulatory/registration framework and guidelines for digital lending (Digital Lending Guidelines, 2022).

Federal Competition and Consumer Protection Commission. (n.d.). FCCPC resources library (FCCPA). https://fccpc.gov.ng/resources-library/fccpa/

Federal Republic of Nigeria. (2011). Evidence Act, 2011. https://placng.org/lawsofnigeria/laws/E14.pdf

Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. https://www.nfiu.gov.ng/images/Downloads/downloads/cybercrime.pdf

Federal Republic of Nigeria. (2018). Federal Competition and Consumer Protection Act, 2018 (FCCPA). https://placng.org/i/wp-content/uploads/2019/12/Federal-Competition-and-Consumer-Protection-Act-2018.pdf

Federal Republic of Nigeria. (2020). Companies and Allied Matters Act, 2020 (CAMA 2020). Official Gazette. https://www.cac.gov.ng/wp-content/uploads/2020/12/CAMA-NOTE-BOOK-FULL-VERSION.pdf

Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023 (NDPA). https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf

Gomez, F., & Ganuza, J. (2020). Mandatory disclosure in consumer contracts: Theory and practice. *Journal of Consumer Policy, 43(1)*, 23-45.

Hacker, P. (2020). Consumer protection in the platform economy: EU and US perspectives. *Journal of European Consumer and Market Law, 9(1)*, 3-11.

Ilobinson, I. K. (2018). Protecting consumers from unfair contract terms in electronic commerce. University of Lagos Institutional Repository. https://ir.unilag.edu.ng/bitstreams/931f7cc8-188f-4d26-a2f0-66f8e46ccc6c/download

Journal of CMSD. (2022). Online dispute resolution: The future of e-commerce in Kenya. https://journalofcmsd.net/wp-content/uploads/2022/05/Online-Dispute-Resolution-The-Future-of-E-Commerce-in-Kenya.pdf

Kanyip, B. (2019). Consumer protection in Nigeria: Law, theory and policy. Law Lords Publications.

KPMG Nigeria. (2023). The Nigeria Data Protection Act, 2023: Summary and commentary. https://assets.kpmg.com/content/dam/kpmg/ng/pdf/the-nigeria-data-protection-act-2023.pdf

Nwauche, E. (2021). Cross-border e-commerce and Nigerian consumer protection law. *African Journal of International and Comparative Law, 29(4)*, 533-553.

Okojie, I. (2020). Corporate accountability under CAMA 2020: New frontiers for Nigerian company law. *University of Benin Law Journal, 16(2)*, 111-139.

Okoye, C. (2022). The future of e-commerce regulation in Nigeria: Between FCCPA 2018 and CAMA 2020. *Journal of Business Law in Africa, 10(1)*, 66-89.

Onakoya, O. O. (2021). E-contracts in Nigeria: Legal issues, challenges and prospects. University of Ibadan Repository. https://repository.ui.edu.ng/items/7a28f094-51f6-4046-a077-6591a6cbe5fl

Oraegbunam, O., & Livinus, L. (2022). Problems of electronic contract in Nigeria today. Legal and Security Journal (LASJURE). https://www.nigerianjournalsonline.com/index.php/LASJURE/article/download/2549/2475

Organisation for Economic Co-operation and Development. (2021). Consumer policy in the digital age. OECD Publishing.

PricewaterhouseCoopers Nigeria. (2021). The rise of Nigeria's digital economy: Opportunities and challenges. PwC Nigeria. https://www.pwc.com/ng/en/assets/pdf/pwc-nigeria-digital-economy.pdf

Templars Law Firm. (2022). Client note: The FCCPC guidelines on digital lending (analysis and summary). https://www.templars-law.com/knowledge-centre/the-fccpc-guidelines-on-digital-lending/

United Nations Commission on International Trade Law. (1996). UNCITRAL Model Law on Electronic Commerce (with Guide to Enactment). https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

United Nations Commission on International Trade Law. (2017). Model Law on Electronic Transferable Records (MLETR). https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf

United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

World Bank. (2020). Doing Business 2020: Comparing business regulation in 190 economies. World Bank.

World Bank. (2024). Responsible digital credit: Protecting customers in digital lending models (Digital Financial Services). World Bank. https://documents1.worldbank.org/curated/en/099072425135514500/pdf/P181316-72eed651-b7c2-4137-a1f0-a00c3e1efede.pdf